Amendments to the Specification:

Please replace the paragraph extending from page 3, line 5 to line 12, with the following rewritten paragraph:

The present invention solves this problem by managing the number of alert indications using a set of decision tables, rules sets, databases, and default conditions. The method receives the alert indications, uses the tables, and rules to determine whether an incident should be declared. The method and system are capable of remembering the alert indications, and identifying patterns in the remembered information in order to properly declare an incident.

Please replace the paragraph extending from page 3, line 18 to line 22, with the following rewritten paragraph:

Yet another object of the invention is a system, which provides the ability to declare ~~and~~ an incident based upon a knowledge base that represents the enterprise administrator's normal methods of correlating and assessing alert streams from a plurality of sources.

Please replace the paragraph extending from page 9, line 6 to line 17, with the following rewritten paragraph:

First, an alert indication is provided at 21. This alert indication can take any form, but it is preferred that the form be a common format information containing one or more alert indications as disclosed in applicant's co-pending application entitled "System And Method For Tracking And Filtering Alerts In An Enterprise And Generating Alert Indications For Analysis," ~~Docket No. 12016-0004~~ U.S. Patent Application Serial No. 10/080,574, filed on Feb. 25, 2002. The co-pending application is hereby incorporated in its entirety by reference. The common format information containing alert indication is preferred since it eases the steps of checking

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

for false positives and for criteria and correlation with specific attack patterns.

Please replace the paragraph extending from page 10, line 21 to page 11, line 5, with the following rewritten paragraph:

If no match occurs, the input 21 is sent to a default processing step 33. This step handles alert indications that may be considered serious but have no specific pattern that would be matched in the rule or decision table checking steps. For example, if the alert indication input 21 is assigned a certain type of threat severity such as a 3 on a scale of 1-5 (1 being the highest threat), the default processing steps checks for a match of the incoming threat severity with the default threat. If the default threat is set at 3, a match would occur and an incident would be then declared at step 29.

Please replace the paragraph extending from page 11, line 6 to line 18, with the following rewritten paragraph:

Once an incident is declared, it can be displayed in any known fashion, including written reports or visual display such as on a computer screen via a web server and a global network, i.e., the internet, or by any of a number of auditory alarms, or by email or pager notifications, or through a server and an internal network. An incident is a correlated collection of alert indications, conclusions, and logged actions ~~take~~ taken by the system or by the operator. It is akin to a breech in the lines during a battle, something requiring the attention of a field commander. Often times, the incident will be based on more than one alert indication over an extended period of time. An incident may not necessarily be specific to a single device or subnet.

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888